ACTIVATING DYNAMIC COUNTERMEASURES TO REDUCE RISK

L. Labuschagne[1]
J.H.P. Eloff[2]
Department of Computer Science, Rand Afrikaans University, P O Box 524,
AUCKLAND PARK 2006, Johannesburg, South Africa

Telephone number:	[1] +27 11 832-3511	[2] +27 11 489-2842
Fax number:	[1] +27 11 832-1050	[2] +27 11 489-2138
Email:	[1] les.labuschagne@pixie.co.za	[2] eloff@rkw.rau.ac.za

Abstract

Conventional risk analysis methodologies are aimed at the identification of suitable countermeasures for specific risks. In the past, many risk analysis methodologies failed to come up to expectations. The analysis of some commercial methodologies identified key problem areas. This paper proposes a categorization method which was used to investigate the recommended countermeasures from various methodologies. The method is based on three categories namely:

* Proactive countermeasures - countermeasures that are implemented and activated before an incident occurs and which are constantly active;
* Dynamic countermeasures - countermeasures that are triggered by an incident;
* Reactive countermeasures - countermeasures that are activated after an incident has occurred.

This paper emphasizes the use of dynamic countermeasures to improve consistency and effectiveness and to reduce cost. The Petri Net modelling method is used to illustrate the difference between the three categories by simulating an actual process. The underlying principle of this article is the importance of having dynamic countermeasures implemented that can either be activated or deactivated, as the case may be. Not only will these countermeasures help to make security measures foolproof, but they will also help reduce the overheads associated with security directly or indirectly.

Keywords

"Proactive countermeasures", "dynamic countermeasures", "reactive countermeasures", "Petri Nets", "IT security", "Internet", "access control", "biometric portfolio".

1. INTRODUCTION

The concept of risk analysis or risk management has always been met with some degree of opposition. Many conventional risk analysis methodologies raised unrealistic expectations, as illustrated in the following statement: "The result of a risk analysis is a set of countermeasures that will combat all risks".

In many cases, the recommendations based on a risk analysis study are made in the form of a bulky report and presented to management. Owing to the fact that managers seldom if ever have time to wade through such voluminous reports, the studying of the risk analysis report is usually delegated to a subordinate. Such subordinate however, invariably lacks both the competence and the know-how to implement the recommendations. The report, therefore, usually ends up lying on a shelf. In other cases, the countermeasures are implemented, but never maintained. Access control mechanisms are implemented, but are either used incorrectly or bypassed by most users. In some cases, a list of countermeasures is produced without consideration for the cost-effectiveness thereof.

Most conventional methodologies recommending the implementation of countermeasures use the asset/threat/countermeasure approach and set boundaries to limit the size of the IT system. IT systems are becoming more open and distributed, and risks are becoming less threatening to assets and merely a threat to the flow of information. Given the fact that technologies such as distributed processing, EDI and work groups are improving in leaps and bounds, it is no longer possible to set bounds to these technologies. Systems are, furthermore, becoming so integrated and interdependent that it is almost impossible to separate them. The flow of information is seldom restricted owing to the fact that there are usually alternative routes that can be followed. It is, therefore, more effective to protect the information rather than the physical asset.

It is, therefore, necessary to analyse the way current methodologies identify and recommend countermeasures so as to establish requirements for state-of-the-art approaches to risk analysis.

The remainder of this article shall be devoted to the following:

i Current methodologies - a high-level overview of countermeasure selection.
ii The categorization of countermeasures - dividing countermeasures into categories to facilitate the process of combination into an optimal solution.
iii The modelling of dynamic countermeasures - to show the difference between dynamic countermeasures and the other categories, as well as the advantages to be derived through the use of a practical example.

The main aim of this article is to show the importance of implementing dynamic countermeasures that can be activated or deactivated, as circumstances may demand. Not only will these measures help improve the effectiveness of security, but they will also directly or indirectly reduce the overheads associated with security.

2. CURRENT METHODOLOGIES

To determine the shortcomings of the latest methodologies, it is vital to analyse the approaches followed, as well as to look at the current perception of implementing countermeasures, as reflected in the literature.

2.1 CRAMM

The acronym "CRAMM" stands for "CCTA Risk Analysis and Management Method", and is used by the UK government [CCTA 93]. The way CRAMM is used to determine suitable countermeasures is to start off with identifying the IT assets. Next, the threats to these assets and the vulnerability of the assets are identified, whereafter a risk value is calculated. This is done by attaching a value to each threat-to-asset pair. Using the latter value and the replacement value of an asset, a risk value can then be calculated to determine exactly how vulnerable an asset is to specific threats.

Measures are then taken to counter the threats in question. Individual countermeasures are selected that are equal to or lower than the calculated risk value of an individual threat. The selected countermeasures are then compared to the implemented countermeasures to highlight any discrepancies. CRAMM does not, however, take into account the cost of countermeasures, except that of a "high, medium, low" value and also does not provide an optimal solution of the least amount of countermeasures needed to counter the largest number of serious risks. A report is then produced with all the threats-to-assets combinations, together with the countermeasures needed to counter them. It is then up to management to decide which threats, according to their risk values, are more serious than others and which countermeasures should be implemented first.

2.2 MELISA

MELISA was developed by the French military in 1984 and has since been commercialised [XPCO 90]. MELISA is based on the principle of eight areas, which are viewed as asset groups. For each of these areas, a number of events can occur. An event is an incident that causes a risk to realize. For each event, there are a number of associated threats. Different threats are linked to different countermeasures on a many-to-many basis, i.e. one countermeasure can be implemented to counter many threats and many countermeasures can be implemented to counter a single threat. Costs are allocated for the implementation of each countermeasure to assist management at the decision-making process. These costs, however, are not used to prioritize countermeasures. They are merely used to assist management in prioritizing countermeasures after management has decided which ones to implement. Furthermore, the residual vulnerability is calculated automatically subsequent to countermeasure implementation. No optimal plan is produced and management must still decide which are the more serious threats, as well as which of the countermeasures will best counteract these threats.

2.3 MARION

MARION was developed as a joint venture between the French insurance industry, the IT industry and the IT security industry [CLUS 94, 88]. MARION starts off by identifying all major threats to the system, as well as the current level of security. Next, the acceptable loss margin of the organisation is determined, together with any constraints that might influence the review. The selection of countermeasures is determined by the available security budget. A decision is then taken, based on the money to be spent on security measures and insurance. Countermeasures are divided into two groups, namely protective and preventative measures. A balance is then struck between the number of countermeasures selected from each group. Countermeasures are selected and prioritized according to the seriousness of the threat they are to combat. A security improvement programme is developed, summarising cost, effect and order of priority of the proposed security improvements. MARION shows what level of security is required, as compared with the existing level of security. A simulation can be done to show how the level of security improves as countermeasures are being implemented.

Current research also reflects the inadequacy of current risk analyses and countermeasure identification methodologies to optimize countermeasure selection. It has become clear that risk analysis needs to change to that of a heuristic approach, according to which risk scenarios can be identified and countermeasures can be recommended according to the scenario, and not according to a specific asset [SOMM 94]. This is especially vital for "softer" risks, for example industrial espionage, in which case losses are difficult to measure and actuarial data is unavailable. Creating a scenario would start off by determining what information is valuable to an outsider and by then identifying where and in what format this information is to be stored.

Research has been done on implementing countermeasures dynamically to prevent certain events from happening [DENA 94]. The two main approaches being researched are detection-by-appearance and detection-by-behaviour. The process being followed starts off by monitoring a network for such events. Once an event has occurred and has been detected, it is interpreted by analysing the characteristics of the "attack". According to these characteristics, the most suitable countermeasures are selected and activated. Detecting the behaviour of a virus would, for instance, activate the appropriate anti-virus software.

After having analysed current literature and various methodologies, it became clear that one of the shortcomings of most risk analysis methodologies is their static approach to utilising countermeasures, i.e. once the countermeasures have been implemented, they are never again reviewed for their effectiveness. It is important, therefore, to analyse the risk when it occurs so that a line of action can be determined.

3. CATEGORIZING COUNTERMEASURES

Countermeasures can be categorized according to different criteria. After having investigated the recommended countermeasures from the CRAMM, MELISA and MARION methodologies, it became clear that countermeasures could be divided into three broad categories. These three categories are proactive countermeasures, dynamic countermeasures and reactive countermeasures.

The reason for this categorization is that proactive countermeasures are, for instance, generally more effective than reactive countermeasures, owing to the fact that recovering from an incident is usually more expensive than preventing it from happening altogether. Dynamic countermeasures, in their turn, tend to be divisible amongst different resources, which factor also has a cost implication. Categorizing countermeasures would, in addition, assist in their selection and combination optimally to provide a comprehensive security plan that is both efficient and cost effective. The three categories can be defined as follows:

3.1 Proactive countermeasures are implemented in an attempt to prevent an incident from occurring. The criterion used to classify a countermeasure as being proactive is whether or not the countermeasure is installed/implemented before an event occurs. The countermeasure is in a permanently active state, which will assist in helping to prevent a certain incident from occurring. A typical example would be the use of passwords. Using passwords for access control purposes would prevent most unauthorised users from accessing a system.

3.2 Dynamic countermeasures are those measures that can either be activated or deactivated, depending on the specific threat. The purpose of dynamic countermeasures is to act on an incident as and when it occurs. The countermeasure is, therefore, not always active, but is triggered by a certain action. The criterion used to classify a countermeasure as being a dynamic one, is whether or not the countermeasure is only used as a result of a threat. The countermeasure must, therefore, already be available for use. In addition, a dynamic countermeasure is one that can be shared amongst many resources. An example of a dynamic countermeasure would be the facility automatically to log off a user once his/her authenticity has become suspect.

3.3 Reactive countermeasures are those measures that are applied after an event has occurred. This category of countermeasures is the least effective of the three, but could help to prevent an incident from recurring. The criterion used to classify a countermeasure as being a reactive one, is whether or not the countermeasure is activated after an event has occurred. Reactive countermeasures are usually inactive and are only activated once an incident has occurred. This would, typically, be auditing all unsuccessful passwords and log-in attempts on a regular basis.

Using the above three categories would assist in grouping countermeasures from different categories to produce an optimal solution. The first line of defence would, naturally, be to prevent an incident from occurring. Proactive countermeasures would be used for this purpose. If these, however, were to fail and the event does occur, the second line of defence would be to control the incident by activating a dynamic countermeasure. If the event can be neither prevented nor controlled, the third line of defence would be to implement a reactive countermeasure in order to analyse the origin of the problem and to prevent it from recurring. However, it is also necessary to determine which countermeasures can be shared among resources. Some countermeasures are not used continuously. They are only used when required. These countermeasures can then be shared by a number of resources and each resource uses it when necessary. This would decrease the number of countermeasures

needed, which would constitute a definite cost saving. Sharing a countermeasure would also reduce the associated overheads, especially those costs incurred through maintenance, which would result in a saving, albeit indirect.

To select countermeasures that complement one another, it is vital to consider additional contributory factors such as cost. Some countermeasures are very effective, but very expensive, for example, to duplicate equipment. It is in these cases that a countermeasure should be shared by different resources, instead of just applying it to one. An example of sharing a countermeasure would be where different servers running different applications are put within one logical domain. This is done so that all communications between this logical domain and the outside world can be controlled. One fileserver can be used for controlling communications and thus only one firewall is necessary to protect all servers within that logical domain. The alternative is that each individual server has its own communications server and firewall, which could be a very expensive solution.

Various methods can be used to illustrate the many uses of countermeasures, but very few clearly show the flow of events and the interdependencies that exist between different components. Of all the methods used to model networks, Petri Nets seems to possess all the characteristics necessary to model dynamic countermeasures.

4. MODELLING DYNAMIC COUNTERMEASURES

In order to illustrate the differences between the three categories of countermeasures, an access control mechanism is modelled, using Petri Nets. Petri Nets is a modelling tool used to represent systems in which concurrent events occur. It is very useful to keep track of these events and to show how they are interlinked. The basic Petri Net theory consists of four components, namely places, transitions, arcs and tokens. For more information on Petri Nets, see [MURA 89].

The example used is one of access control to an application. The user is identified and authenticated in parallel. This is done by using a log-in name and password to identify the user and a typing biometric to authenticate the user. A typing biometric is the speed at which a user types, as well as the time lapse between each key being struck. Other factors can also be included, for example combination of characters typed and typing style used. Once a user has been allowed access to the application, he/she is continuously monitored to ensure his/her authenticity. The example can be graphically illustrated as on the next page.

A user enters his/her log-in name and password. The log-in name and password are verified, which either gives the user access to the application or logs the incorrect attempt. The user gets three chances to enter the correct log-in name and password before being locked out. Once the user has been locked out, the system administrator is the only person who can reinstate such user as an authorised user.

While the user is logging in, a biometric portfolio is being determined for him/her. A biometric portfolio consists of, for example, measuring the typing biometric of a user during a typing session.

Once the user has been authorised to proceed, a timer is activated. Should the user not be actively using the application for a certain period of time, he/she would be automatically logged out. If the user does use the application, he/she is only allowed to do so for a limited period of time without a valid biometric portfolio. If the set time expires without a valid biometric portfolio having been determined, the user is prompted to re-enter his/her password and log-in name. While the user is using the application, two more attempts are made to determine a biometric portfolio. These attempts to determine a biometric portfolio result in one of the following:

(a) Biometric portfolio timed out - after a certain period of time, no biometric portfolio could be determined
(b) Biometric portfolio declared invalid - the biometric portfolio does not match previous biometric portfolios for that user
(c) Biometric portfolio declared valid - a successful biometric portfolio has been determined and matches previous biometric portfolios.

Once a valid biometric portfolio has been established, the time limit for using the application falls away. However, while the user is using the application, his/her biometric portfolio is constantly redetermined and compared, to determine if it is still the same user as the one that logged in. Should a discrepancy be picked up, the user is automatically logged out and the incident is reported in an audit report.

From this example, it is possible clearly to show the differences between the three types of countermeasures. The proactive countermeasures are the password and log-in mechanisms and the biometric portfolio determination and comparison functions. These are proactive because they are used before an undesired event occurs and also because they are constantly active.

The "automatic log-out" owing to a change in the biometric portfolio of a user is an example of a dynamic countermeasure. The automatic log-out function is passive until an undesired event occurs, whereupon the countermeasure is activated dynamically. It is, therefore, possible to put an end to an undesired event as it is occurring. Furthermore, this countermeasure can be used for all users and applications across all platforms. This would indirectly reduce the cost of security, thanks to cheaper maintenance, as well as the ease with which these countermeasures can be implemented and maintained.

The reactive countermeasure is activated when the incorrect log-ins and automatic log-outs are analysed. Once a week, the security administrator will go through the audit reports generated to determine any abnormal behaviour or any possible security breaches that might have occurred. This countermeasure is passive and is, therefore, only activated once the event has already occurred. From this, it is possible to concentrate on a specific user's activities or implement countermeasures to prevent a certain incident from recurring.

5. CONCLUSION

Implementing security in big organizations can be a very expensive undertaking. For this reason, it is necessary to find a cost-effective solution that still provides maximum protection.

By using the categorising scheme proposed in this article, it is possible to distinguish between different types of countermeasures and to find an optimal solution by combining complementary countermeasures, as well as by sharing expensive countermeasures amongst different resources.

Extensive research has been undertaken on information technology risk analysis. The methods used have evolved over time, incorporating much experience. The main object of the present article is not to change the way in which information technology risk analysis is being performed, but rather to help "fine-tune" it. The biggest problem still seems to lie in justifying the recommended countermeasures. Even though it is possible to justify the list od such measures by performing a cost benefit analysis, it is hard to justify the effectiveness thereof. Most sets of recommended countermeasures are, however too cumbersome to be implemented in practice, with the result that these countermeasures often have to be prioritized and that cut-off points are dictated by budgetary constraints. This leads to the fact that, although the selected countermeasures are the more effective ones, they were initially prioritized on an individual basis. The overall effectiveness of the selected countermeasures are, therefore, compromised. It is possible, according to the above categorization method, to combine a number of countermeasures to be even more effective than the same number of countermeasures selected from the prioritized list.

Although technological advances are made in leaps and bounds, the methods used to analyse risks and identify countermeasures remain unchanged. Future research would, therefore, be aimed at adapting risk analysis methodologies to identify and more effectively to implement countermeasures to secure these new technologies.

Possible research would include developing a prototype, knowledge-based, risk analysis tool that would place more emphasis on identifying and recommending countermeasures. These countermeasures will be categorized according to the above scheme. Each countermeasure will then be weighed according to the category to which it resorts in order to compare the effectiveness and cost impact of these countermeasures. Dynamic countermeasures are the most effective and would be allotted the highest weight. Proactive countermeasures are, for example, more effective than reactive ones and would be allotted a medium weight. Reactive countermeasures are the least effective and would, therefore, be allotted the lowest weight. The weightings would be relative to one another and not fixed according to specific criteria. Countermeasures that complement one another can be linked together to improve the overall effectiveness thereof. Using a countermeasure from each category to counter the same risk would, at best, greatly reduce the probability of that risk occurring and, at worst, soften the impact it would have. When a risk is identified, the most effective countermeasure is selected to reduce it. All countermeasures linked to that specific countermeasure will be selected. Together, they will form a group of countermeasures. Each countermeasure group would consist of all three categories of countermeasures. Each selected countermeasure will, in turn, be checked to determine whether or not it corresponds with any of the remaining risks.

When determining the recommended countermeasures, it is important to include countermeasures from each category in order to cover a wider spectrum of risks and their associated impacts. Greater emphasis will, therefore, be placed on dynamic countermeasures, due to their greater effectiveness.

REFERENCES

[BADE 94] Karin P. Badenhorst, Jan H.P. Eloff (1994), TOPM: A formal approach to optimization of information technology risk management, p.411 - p.435, *Computers & Security*; Volume 13 Number 5, Elsevier Science Ltd.

[CCTA 93] CCTA (1993), The CCTA Risk Analysis and Management Method (CRAMM) User Guide, Version 2.1, CCTA.

[CLAS 94] Alison Classe (1994), Hazard Warning, p.568, *Computers & Security*; Volume 13 Number 7, Elsevier Science Ltd.

[CLUS 94] CLUSIF (1994), Management of the Information Security Master Plan - MARION, CLUSIF, Paris.

[CLUS 88] CLUSIF (1988), Les Projects Prioritaires arpes le Schema Directeur Security, CLUSIF, Paris.

[DENA 94] Micheal Denault, Dimitris Gritzalis, Dimitris Karagiannis, Paul Spirakis (1994), Intrusion detection: approach and performance issues of the SECURENET system, p.495 - p507, *Computers & Security*; Volume 13 Number 6, Elsevier Science Ltd.

[GATZ 94] Stella Gatziu, Klaus R. Dittrich (1994), Detecting composite events in active database systems using Petri Nets, Proc. of the 4th Intl. Workshop on research issues in Data Engineering: Active Database Systems, Houston, Texas.

[MURA 89] Tadao Murata (1989), Petri Nets: Properties, Analysis and Applications, *Proc. of the IEEE*, Vol. 77 No. 4, p.541 - p.580.

[SHAR 94] Ronald Sharp, Steven Eisen (1994), Network security in a heterogeneous environment, p.489, *Computers & Security*; Volume 13 Number 6, Elsevier Science Ltd.

[SOMM 94] Peter Sommer (1994), Industrial Espionage: Analysing the Risk, p.558 - p.563, *Computers & Security*; Volume 13 Number 7, Elsevier Science Ltd.

[SUND 94] Chris Sundt (1994), Putting your information on a network creates new security problems, p.488, *Computers & Security*; Volume 13 Number 6, Elsevier Science Ltd.

[SYMO 94] Ian M. Symonds (1994), Security in Distributed and Client/Server Systems - A Management View, p.473 - p.480, *Computers & Security*; Volume 13 Number 6, Elsevier Science Ltd.

[XPCO 90] XP Conseil (1990), The MARION and MELISA Methods, XP Conceil, Paris.

AUTHOR BIOGRAPHIES

Les Labuschagne

Les Labuschagne received his M.Com Informatics degree cum laude in 1992 specialising in Information Technology Risk Analysis. He has been involved in Information Technology since the beginning 1992. Current research is aimed at obtaining a D.Com degree in Information Security (informatics) at the Rand Afrikaans University in South Africa. He is a member of the Computer Society of South Africa (CSSA) and an associate of the Society of Risk Managers of South Africa. He is involved in presenting Information Technology Risk Management seminars on a regular basis and have been invited to talk at numerous local conferences. He is currently involved in Information Technology Risk Management Consultancy to a number of large South African corporates.

Prof Jan Eloff

Jan Eloff holds a Ph.D in information security (computer science). His involvement in information security started in the early 1980's. Previously he worked in Anderson Consulting and a large chemical concern. Currently he is a professor in computer science at the Rand Afrikaans University in South Africa. He has published a number of research papers in internationally accredited journals. During 1994 he was invited to serve as a guest professor at the Institute for Informatics, University of Zurich in Switzerland. He is the chairman of the Information Security Special Interest Group in South Africa (affiliated to the Computer Society of South Africa (CSSA)). In 1995 he was elected chairman of the International Workgroup on Small Systems Security (WG11.2) which is affiliated to the International Federation for Information Processing (IFIP). He was programme chairman for the Eleventh International conference on Information Security (IFIP/SEC '95).